BPC Platform Operations / Deprecated

ur Rating: ☆☆☆☆☆
Results: ☆☆☆☆☆

Share

Key Vault Access Procedure

Created by Nathan Mitten
Last updated: Nov 19, 2021 • 3 min read • 14 people viewed

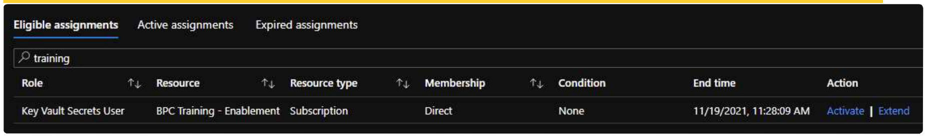
Purpose

The following document will describe how to access a Key Vault which utilizes role-based access control rather than Access Policies. In the table below under 4.a Automation Devs will use steps under i and ops will use steps under ii.

PIM Requests

When needing to access a customer's key vault, you will need to perform an additional PIM request for Key Vault Secrets User.

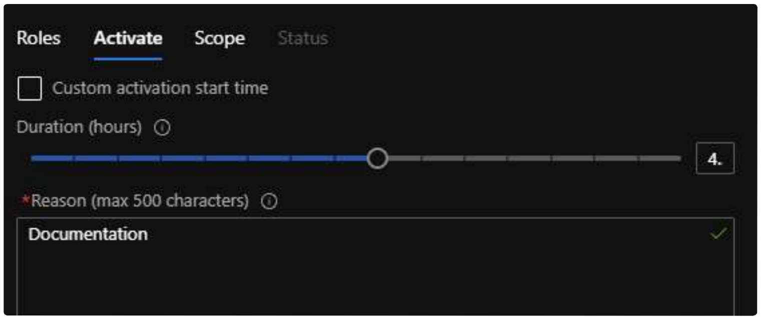
1. Browse to Privileged Identity Management in the Azure Portal
2. Click My roles
3. Click Azure resources
4. Find the Key Vault Secrets User role - How this is done can vary by assignment and how the role is searched for.
    a. Under Eligible assignments search for either the specific Subscription Name or "Key Vault" and note the Resource and Resource Type
        i. For Resource Type Subscription follow the below - **Automation Devs** will typically use this method (note the screen shot below I have searched for the specific Subscription not the role).



training

Role	Resource	Resource type	Membership	Condition	End time	Action
Key Vault Secrets User	BPC Training - Enablement	Subscription	Direct	None	11/19/2021, 11:28:09 AM	Activate | Extend

1. Click Activate on the role
2. Provide a reason and adjust the duration as needed

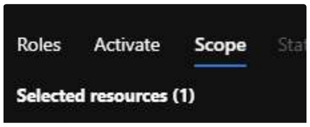


□ Custom activation start time

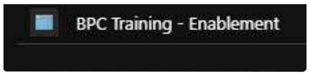
Duration (hours) 4.

*Reason (max 500 characters): Documentation

3. Click the Scope Button to confirm the Subscription required is listed under Selected resources

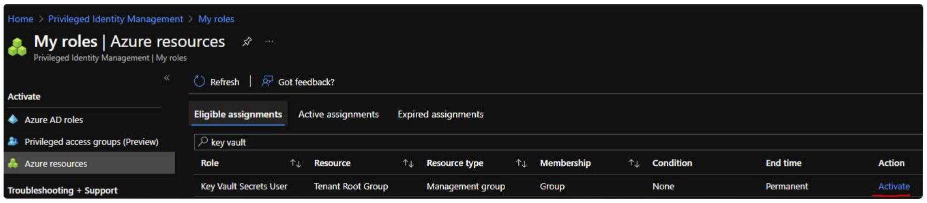


Selected resources (1)


BPC Training - Enablement

4. Once confirmed click Activate

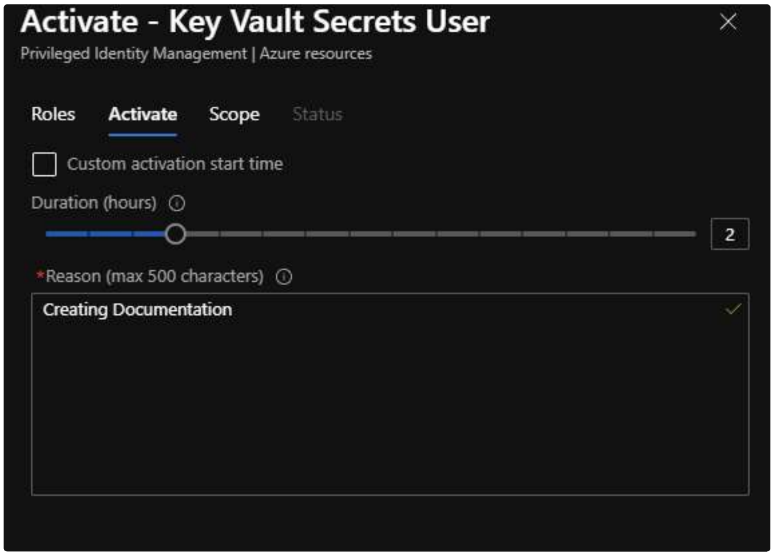
ii. For Resource Type Management Group follow the below - **Operations** will typically use this method


Home > Privileged Identity Management > My roles
My roles | Azure resources
Privileged Identity Management | My roles
Refresh
Got feedback?
Activate
Azure AD roles
Privileged access groups (Preview)
Azure resources
Troubleshooting + Support
Eligible assignments
Active assignments
Expired assignments

key vault

Role	Resource	Resource type	Membership	Condition	End time	Action
Key Vault Secrets User	Tenant Root Group	Management group	Group	None	Permanent	Activate

1. In the fly out box, adjust the duration as needed and provide a reason for the request


Activate - Key Vault Secrets User
Privileged Identity Management | Azure resources
Roles
Activate
Scope
Status

□ Custom activation start time

Duration (hours): 2

*Reason (max 500 characters): Creating Documentation

2. Click the scope tab

3. Click the blue select scope button

4. Search for the subscription you require and click it so it appears under selected resources

5. Click Activate - failure to scope to a subscription level will have the request be denied.

Notable Subs with Access Policies

The following subscriptions are exceptions that have not had their KV's converted at this moment.

- Sandvik
- BPC Live Services
- Support Internal
- Pen Tests

Future Plans

Currently there is a technical limitation whereby we cannot create a custom role that has the Key vaults secrets user data actions and combine it with the JIT role. Once this limitation is resolved by Microsoft (no ETA) the two roles will be combined and the need to perform the above PIM request specifically for KV Secrets User will be no longer required.

Like Ibrahim Ali likes this

No labels